Departamento de Engenharia Informática e de Sistemas
Instituto Superior de Engenharia de Coimbra

Licenciatura em Engenharia Informática

Segurança 2020/2021

Configuração Avançada de um Equipamento

Diogo Costa - 2018016581

Filipe Oliveira - 2018018618

Nuno Aparício - 2014014661

Índice

Índice de Figuras

Índice de Tabelas

Topologia

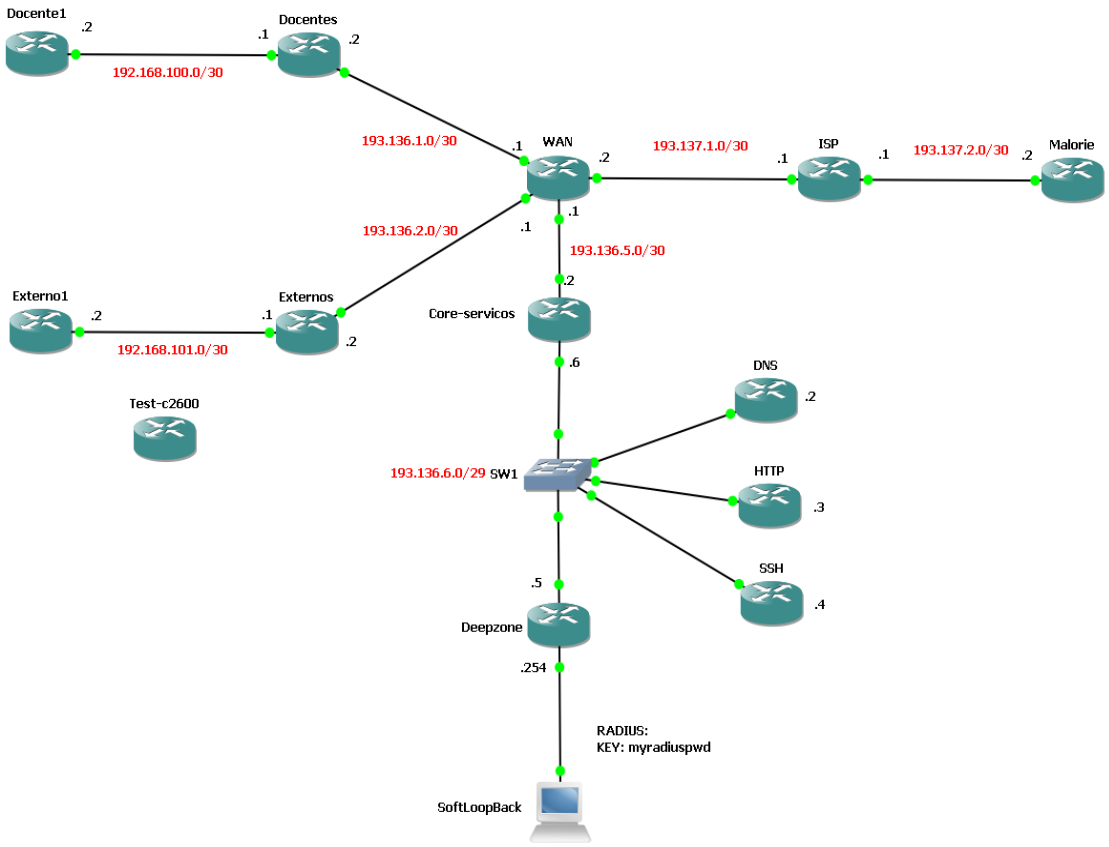

Figura 1 Topologia

Introdução

Neste trabalho prático, o objetivo principal é conseguir estimular a aplicação prática dos conhecimentos adquiridos no âmbito das aulas de segurança, assim como promover a pesquisa de soluções técnicas que promovam as melhores práticas de segurança em redes.

Relativamente aos routers utilizados, foram utilizados apenas routers 7200 devido a ter problemas sendo todos os comandos do router Externos testados num router 2600 para verificar a sua compatibilidade. Seguem-se os IP's de cada router.

Externo1	f0/0: 192.168.101.2
Externos	f0/0: 193.136.2.2 f0/1 :192.168.101.1
Docente1	f0/0: 192.168.100.2
Docentes	f0/0: 193.136.1.2 f0/1 :192.168.101.1
WAN	e1/1: 193.136.2.1 e1/3:193.136.1.1 e1/0: 193.136.5.1 f0/0: 193.137.1.2
ISP	f0/0: 193.137.2.1 f0/1: 193.137.1.1
MALORIE	f0/0: 193.137.2.2
Core-Servicos	f0/0: 193.136.5.2 f0/1: 193.136.6.6
DNS	f0/0: 193.136.6.2
HTTP	f0/0: 193.136.6.3
SSH	f0/0: 193.136.6.4
DeepZone	f0/0: 193.136.6.5 f0/1: 192.168.200.254
SoftLoopback	192.168.200.2

Tabela 1 Endereços

Utilizadores

Routers

Nome de Utilizador	Password
oper	operpwd
adm	admpwd
manager	manpwd

Tabela 2 Utilizadores dos routers

Routers de VPCS

Nome de Utilizador	Password
oper	operpwd

Tabela 3 Utilizadores de VPCS

A password do Enable em todos os equipamentos é “myenapwd”.

Telnet & SSH

Apenas dois routers possuem telnet nomeadamente o Externos, devido a este ser um router c2600 e não aceitar SSH, e o WAN pois foi necessário para a implementação da ACL Dynamic. Como o protocolo de aplicação telnet é pouco seguro decidimos aplicar nos restantes routers SSH e bloquear o telnet.

Ao reiniciar a topologia, a key de SSH não é guardada. Para que possa ser feito SSH aos equipamentos é necessário gerar a key nos equipamentos que o permitem com o seguinte comando:

crypto key generate rsa general-keys modulus 1024

Rotas

O Router WAN tem rota default para sair para o router ISP.

WAN tem uma rota para a rede de Docentes, Externos e Core-Servicos.

Core-Servicos tem rotas para a WAN, rede abaixo (193.136.6.0/29) e rotas de saída para o ISP.

Relativamente ao Router Deepzone apenas tem rotas de saída.

AAA e Logging

Configuração do Radius

Para esta configuração resolvemos usar o Radius que é um protocolo que opera nas portas 1812 e 1813, que fornece a autenticação centralizada, a autorização e a gestão contabilística (AAA) para os utilizadores que se ligam e utilizam o serviço de rede. A sua

principal função é autenticar utilizadores. Com a autenticação AAA, vai permitir que o Administrador da rede consiga configurar e acessar o dispositivo.

Usámos o radius nos routers Deepzone, Core-serviços, Wan, Externos e Docentes. Sempre que exista uma autenticação realizada com sucesso ou falhada o Radius mostrará essa informação.

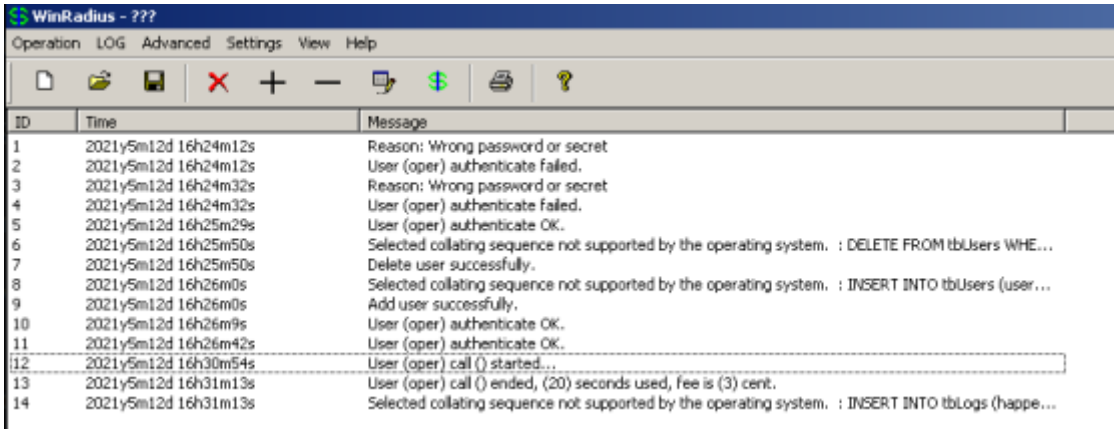

Figura 2 WinRadius

```
Deepzone(config)#do show run | i aaa
aaa new-model
aaa authentication login default local group radius
aaa authorization exec default local
aaa accounting exec default start-stop group radius
aaa session-id common
Deepzone(config)#
```

Figura 3 Configuração AAA

A key utilizada para o servidor radius é “myradiuspwd”.

```
radius-server host 192.168.200.2 auth-port 1812 acct-port 1813 key myradiuspwd
```

Figura 4 Configuração Radius

Configuração do Syslog

O Servidor de syslog foi configurado no IP 192.168.200.2.

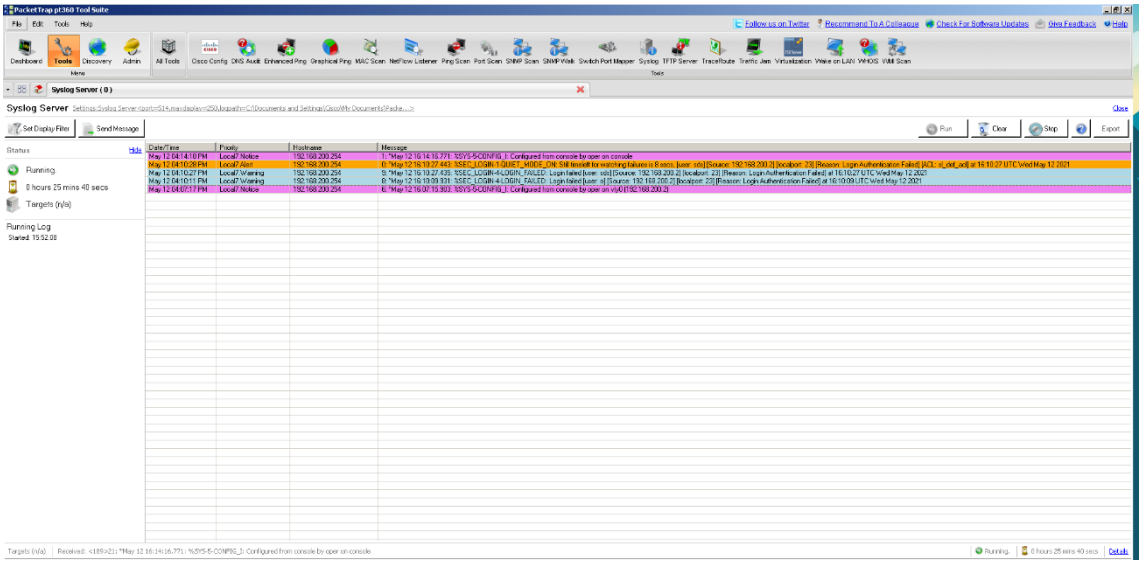

Figura 5 Ambiente de Syslog

A configuração do Syslog foi realizada nos routers Deepzone, Core-serviços, WAN, Externos e Docentes. Foi ativado o log de sucesso e insucesso do login.

```
login on-failure log
login on-success log
```

Figura 6 Log de login

Configurações básicas de segurança

Banners

Sempre que for iniciado um router aparecerão dois banners no qual serão indicadas algumas informações básicas.

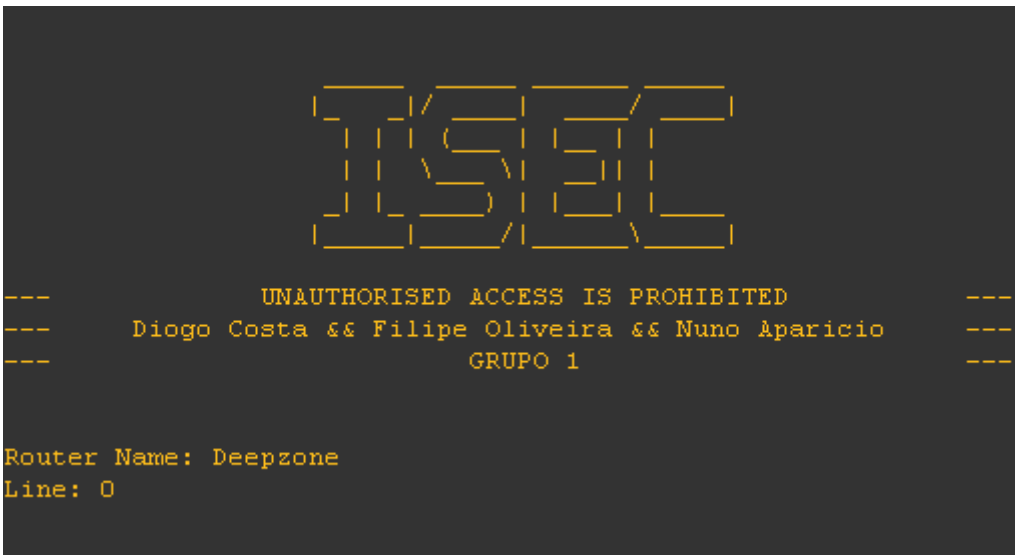

Figura 7 Banner MOTD e Login

Seguidamente o utilizador terá de fazer login, em que posteriormente aparecerá os IPs que cada interface tem.

```
Interfaces:
f0/0: 193.136.6.5
f0/1: 192.168.200.254
```

Figura 8 Banner EXEC

Restrições nos inicios de sessão

No caso de se enganar a iniciar sessão num router haverá um bloqueio de 10 minutos e prazo de 1 minuto no caso de falhar 3 tentativas de acesso.

```
login block-for 600 attempts 3 within 60
```

Figura 9 Bloqueio de tentativas

Privilégios de administração

```
username manager privilege 15 secret 5 $1$TsIA$TB9.LTdN4Gkyzob2CqV8V1
username adm privilege 5 view deny-shutdown secret 5 $1$rI/S$sGyaTd85.qHdilQYsNVOJ1
username oper view permit-descritivo secret 5 $1$7TO3$UqSltVoOaGsdaV9qi.BuH.
```

Figura 10 Privilégios de Utilizador

```
privilege interface level 15 shutdown
privilege configure level 0 interface
privilege exec level 0 configure terminal
privilege exec level 0 configure
privilege exec level 5 show ip interface
privilege exec level 5 show ip
privilege exec level 5 show
```

Figura 11 Configuração de privilégios

No router Externos não foram realizadas as restrições pois o router 2600 não suporta vistas.

Utilizador Operador (oper)

Este utilizador apenas pode aceder à interface de dentro e alterar a sua descrição. Como este só tem permissões para isto deixámos a possibilidade de ser realizado um “show running-config”.

```
parser view permit-descritivo
 secret 5 $1$hHmt$WFhdKB44ov6uqOxzHGfHs0
 commands interface include description
 commands configure include interface
 commands exec include configure terminal
 commands exec include configure
 commands exec include show running-config
 commands exec include show
 commands configure include interface FastEthernet0/1
```

Figura 12 Permissões do oper

Utilizador Administrador (adm)

Este utilizador pode fazer as alterações que quiser nas interfaces sendo que apenas não pode ligar ou desligar as mesmas. O mesmo, pode também verificar as informações acerca das interfaces.

```
parser view deny-shutdown
 secret 5 $1$Qo4g$P.xfoxoFmBMU/pOxV9wv0.
 commands interface exclude shutdown
 commands configure include all interface
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show interfaces
 commands exec include show
```

Figura 13 Permissões adm

Utilizador Gestor (manager)

Este utilizador como tem controlo total sobre o equipamento, foi apenas definido que tem o nível de privilégio 15.

Configuração das Firewalls

Anti-spoofing a partir da internet

Para impedir o spoofing vindo do exterior bloqueamos todos os dados vindos da rede Malorie (Restrição 30).

```
Extended IP access list f0/0-in
    10 permit tcp host 193.137.2.2 host 193.137.1.2 eq telnet
    20 Dynamic users permit icmp host 193.137.2.2 host 193.136.6.2
    30 deny ip 193.137.2.0 0.0.0.255 any
    40 permit ip any any
```

Figura 14 ACL Spoofing

Anti-spoofing e RFC1918 para a internet

Para resolver este problema criamos uma ACL standard em que negamos a passagem de dados de IPs Privados(RFC1918).

```
Standard IP access list f0/0-out
    10 deny   192.168.0.0, wildcard bits 0.0.255.255
    20 deny   10.0.0.0, wildcard bits 0.255.255.255
    30 deny   172.16.0.0, wildcard bits 0.15.255.255
    40 deny   224.0.0.0, wildcard bits 31.255.255.255
    50 deny   127.0.0.0, wildcard bits 0.255.255.255
    60 permit any
```

Figura 15 Anti-Spoofing e RFC1918

TIME-BASED

Aplicámos a ACL TIME-BASED, para definir o período em que os utilizadores tenham a permissão de aceder à internet. Não sendo permitido qualquer ligação do exterior para estas redes.

O comando para configurar a ACL, baseada no tempo, é o time-range. Usado para especificar o período de tempo em que a declaração ACL é válida.

```
Extended IP access list f0/0-out
    5 deny ip 193.136.1.0 0.0.0.3 host 193.137.1.1 time-range FIM-SEMANA (inactive)
```

Figura 16 Aplicação de time-range a uma ACL

Ao executar este comando, é colocado no modo de configuração da lista de acesso no qual especificamos um intervalo de tempo periódico em que é bloqueado o acesso das 0h00m às 23h59m ao fim de semana.

```
time-range FIM-SEMANA
 periodic weekend 0:00 to 23:59
!
```

Figura 17 Configuração time-range

A declaração da lista de acesso só será processada quando a hora do router se enquadrar dentro do período especificado.

Reflexive

Ao utilizar a access-list reflexive, o router acompanhará as ligações de saída e permitirá automaticamente o tráfego de retorno.

Para começar criámos uma access-list que vai permitir o telnet apenas através do soft-loopback.

```
Extended IP access list f0/0-in
    10 permit icmp any any
    40 deny ip 193.136.0.0 0.0.255.255 any
    50 permit tcp host 192.168.200.2 any eq telnet reflect reflexive-acl (15 matches)
    60 deny ip any any (10 matches)
```

Figura 18 Configuração da ACL Reflected

Depois de realizarmos um telnet a lista de acesso, esta irá criar a seguinte lista de acesso.

```
Reflexive IP access list reflexive-acl
    permit tcp host 193.136.2.2 eq telnet host 192.168.200.2 eq 2824 (15 matches) (time left 296)
```

Figura 19 ACL Reflected

CBAC

O CBAC é capaz de verificar até a camada 7 do modelo OSI (Aplicação) e pode criar regras dinâmicas para permitir o tráfego de retorno. É semelhante à lista de acesso reflexive, mas uma das principais diferenças é que a ACL reflexive apenas verifica até à camada 4 (Transporte).

Primeiramente definimos os pacotes que queremos dar Inspect e assim permitir o ICMP com o CBAC.

```
ip inspect name CBAC icmp
```

Figura 20 Permissão ICMP com CBAC

E por fim definimos a interface que queremos que o CBAC atue.

```
interface FastEthernet0/1
 ip address 192.168.100.1 255.255.255.25
 ip access-group f0/1-in in
 ip access-group f0/1-out out
 ip nat inside
 ip inspect CBAC out
 ip virtual-reassembly in
 duplex auto
 speed auto
```

Figura 21 Atribuição CBAC na Interface

O CBAC teve de ser usado na rede Docentes devido aos routers c2600 não o permitirem.

Dynamic

Para permitir que o Malorie consiga pingar o servidor DNS foi criado um access-list dynamic para que, ao fazer telnet e entrar com as credenciais do myaccess o mesmo ira perder conexão e ativar o ICMP do Malorie para o DNS. Esta ligação de ICMP dura apenas 2 minutos.

```
Extended IP access list f0/0-in
    10 permit tcp host 193.137.2.2 host 193.137.1.2 eq telnet
    20 Dynamic users permit icmp host 193.137.2.2 host 193.136.6.2
    30 deny ip 193.137.2.0 0.0.0.255 any
    40 permit ip any any
```

Figura 22 Configuração Dynamic na ACL

Foi criado o utilizador myaccess com o comando "autocommand" para que este ative a dynamic.

```
username myaccess secret 5 $1$ACVE$Q8tQ/Clgd/JbFj5GB/OY5O
username myaccess autocommand access-enable host timeout 2
```

Figura 23 Utilizador myaccess

Por aconselhamento do professor a ZBF deve ser aplicada no router core-serviços. Por consequência a ZBF não é compatível com a extended na mesma interface e como tal decidimos criar a dynamic na WAN permitindo assim o ping para o DNS a partir do Malorie.

Zone-based

Na firewall Zone-Based a ideia é não atribuir listas de acesso a interfaces, mas criar diferentes zonas. Nas interfaces serão atribuídas as diferentes zonas e as políticas de segurança serão atribuídas ao tráfego entre as mesmas.

Primeiramente foi criada uma access-list extended numerada que será aplicada nas zonas criadas.

```
Extended IP access list 101
    10 permit tcp any host 193.136.6.2 eq domain
    20 permit tcp any host 193.136.6.3 eq www
    30 permit tcp any host 193.136.6.4 eq 22
    40 permit udp 192.168.0.0 0.0.255.255 any
    50 permit tcp 192.168.0.0 0.0.255.255 any (6 matches)
    60 permit udp 193.136.0.0 0.0.255.255 any (1113 matches)
    70 permit icmp any any (2806 matches)
```

Figura 24 ACL atribuída nas diferentes zonas

De seguida foram criadas 2 zonas.

```
zone security F0/0
 description externa
zone security F0/1
 description zona dmz
```

Figura 25 Criação de zonas

O próximo passo foi atribuir as zonas às interfaces adequadas.

```
interface FastEthernet0/0
 ip address 193.136.5.2 255.255.255.252
 zone-member security F0/0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 193.136.6.6 255.255.255.248
 zone-member security F0/1
 duplex auto
 speed auto
```

Figura 26 Atribuição das Zonas às Interfaces

De seguida criamos as classes e atribuímos as respetivas access-lists a cada uma das classes.

```
class-map type inspect match-all f0/0-class
 match access-group 101
class-map type inspect match-all f0/1-class
 match access-group 101
```

Figura 27 Criação das Classes e atribuição das ACL's

Depois criamos a policy-map e demos permissão para o “inspect” de cada uma das classes

```
policy-map type inspect f0/0-policy
 class type inspect f0/0-class
  inspect
 class class-default
  drop
policy-map type inspect f0/1-policy
 class type inspect f0/1-class
  inspect
 class class-default
  drop
```

Figura 28 Criação Policy-map e atribuição das classes

Por fim definimos a nossa “zone-pair” atribuindo as zonas de source e destination. Demos também permissão à policy criada anteriormente.

```
zone-pair security f0/0-f0/1 source F0/0 destination F0/1
 service-policy type inspect f0/0-policy
zone-pair security f0/1-f0/0 source F0/1 destination F0/0
 service-policy type inspect f0/1-policy
```

Figura 29 Criação da Zone-Pair

Configuração do NAT

Ao configurar o NAT permitimos às redes privadas que utilizam endereços IP não registados se conectem à Internet. O NAT opera nos Routers Externos e Docentes, e traduz os endereços privados na rede interna em endereços legais, antes de os pacotes serem encaminhados para outra rede.

Por exemplo, a rede externos (192.168.101.0/30) envia um pacote para a rede externa. Sem a configuração do NAT este pacote sairia com o IP privado. Ao aplicar o NAT no router "externos" definimos que todos os pacotes que saiam da rede 192.168.101.0 saia com o IP público. Este IP está presente na interface f0/0 do router Externos. O mesmo se aplica para a rede Docentes.

1º Define-se quais as interfaces de saída e de entrada.

```
interface FastEthernet0/0
 ip address 193.136.1.2 255.255.255.252
 ip access-group f0/0-in in
 ip access-group f0/0-out out
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.100.1 255.255.255.252
 ip access-group f0/1-in in
 ip access-group f0/1-out out
 ip nat inside
 ip inspect CBAC out
 ip virtual-reassembly in
```

Figura 30 Atribuição de Outside e Inside nas Interfaces

2º Em seguida, configurámos uma ACL que inclui uma lista dos endereços de origem internos que serão traduzidos.

```
Standard IP access list 1
    10 permit 192.168.100.0, wildcard bits 0.0.0.255
```

Figura 31 ACL de IP's Privados

3º Por fim, ativamos o NAT.

```
ip nat inside source list 1 interface FastEthernet0/0 overload
```

Figura 32 Configuração do NAT na Interface f0/0

Conclusão

Baseado no que acabámos por realizar neste trabalho prático, uma pessoa com conhecimentos básicos de GNS3 e CISCO, conseguirá através deste relatório espelhar na sua imagem Windows XP exatamente os mesmos procedimentos que nós utilizámos e assim entender mais acerca de serviços de segurança com aplicação de firewalls, logging, autenticação, autorização bem como a configuração do NAT.